IN THE CLAIMS

Amend claims 1, 14, and 17 as follows:

1. (currently amended): A method of determining validity of a transaction carried out by a user at a data processing system, the method including the steps of:

a) receiving a user identification card and a first entry of data from the user;

b) checking the first entry of data against a first stored field of security data;

c) issuing a message to the user which requests a subset entry, consisting of less than all characters of a second stored field of security data, and receiving the subset entry from the user;

d) checking the subset entry against the corresponding subset within the second stored field of security data; and

e) executing a computer program via the data processing system to determine ~~determining~~ the validity of the transaction based upon the results of the checks of steps (b) and (d).

2. (original): A method according to claim 1, further comprising the step of:

f) displaying the first and second entries of data after receiving the second entry of data.

3. (canceled)

4. (original): A method according to claim 3, wherein one entry of data is a personal identification number (PIN) associated with the user identification card and the other entry of data is data personal to an authorized holder of the card.

5. (original): A method according to claim 4, wherein at least one of the first and second stored fields of security data is stored on the user identification card.

PAGE 5/10 * RCVD AT 12/14/2004 9:47:44 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:937 445 6794 * DURATION (mm-ss):03-50

6. (previously presented): A data processing system for carrying out a transaction by a user of the system, the data processing system comprising:

manual data entry means for allowing the user to enter data;

communication means for communicating information to the user;

a data processing unit for

(i) controlling the communication means to request a first entry of data from the user via the data entry means,

(ii) checking the first entry of data against a first stored field of security data,

(iii) controlling the communication means to request a second entry of data containing a specified subset of less than all digits of specified security data from the user via the data entry means,

(iv) checking the second entry of data against a subset of a second stored field of security data, and

(v) determining the validity of the transaction based upon results of the checks made of the first and second entries of data against the first and second stored fields of security data, respectively.

7. (original): A data processing system according to claim 6, wherein the communication means includes visual display means for displaying the results of checking the first and second entries of data.

8. (original): A data processing system according to claim 7, wherein the data processing unit causes the communication means for make at least one further request for data to be entered by the user through the data entry means when an incorrect entry of data is received, and then checks the data entered in response to the further request against stored security data.

PAGE 6/10 * RCVD AT 12/14/2004 9:47:44 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:937 445 6794 * DURATION (mm-ss):03-50

9. (original): A data processing system according to claim 8, wherein the nature of a further request for data is determined by the nature of the error or errors in the data previously received from the user via the data entry means.

10. (original): A data processing system according to claim 8, further comprising a card reader for reading data from a user identification card inserted by the user into the card reader for the purpose of initiating a transaction.

11. (original): A data processing system according to claim 10, wherein the data processing unit causes the card reader to capture the user identification card when an error in the data is received in response to a final request.

12. (original): A data processing system according to claim 11, wherein the card reader reads at least one of the stored fields of security data from the user identification card.

13. (original): A data processing system according to claim 5, wherein the data processing unit keeps a record of the requested second entry of data.

14. (currently amended): A method of validating identity of a party attempting to execute a transaction, comprising the following steps:

a) accepting an identity card from the party;

b) reading first and second data from the card;

c) prior to asking for any other identity data, presenting a message asking the party to enter the first data; and

d) executing a computer program to compare ~~comparing~~ the first data entered with the first data read from the card and, if they agree, presenting a message asking the party to enter the second data; and

PAGE 7/10 * RCVD AT 12/14/2004 9:47:44 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:937 445 6794 * DURATION (mm-ss):03-50

e) executing the computer program to compare ~~comparing~~ the second data entered with the second data read from the card and, if they agree, proceeding with the transaction.

15. (previously presented): Method according to claim 14, in which the first and second data are stored in the card in encrypted form.

16. (previously presented): Method according to claim 14 and, wherein lack of agreement between an entered data and a data read from the card suspends the transaction.

17. (currently amended): A method of validating identity of a party attempting to execute a transaction, comprising the following steps:

a) accepting an identity card from the party;

b) reading first and second encrypted data from the card;

c) presenting a message asking the party to enter the first data; and

d) executing a computer program to compare ~~comparing~~ the first data entered with the first data read from the card and, if they agree, presenting a message asking the party to enter the second data; and

e) executing the computer program to compare ~~comparing~~ the second data entered with the second data read from the card and, if they agree, proceeding with the transaction

f) suspending the transaction if the second data entered fail to agree with data read from the card, and evaluating whether lack of agreement results from a keying error, or from guessing.

18. (previously presented): Method according to claim 1, wherein, at a later time, the user presents the identification card again, in connection with a different transaction, and method includes the step of

PAGE 8/10 * RCVD AT 12/14/2004 9:47:44 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:937 445 6794 * DURATION (mm-ss):03-50

f) issuing a message requesting entry of a second subset entry, consisting of a different subset of said second stored field of security data.

19. (previously presented): System according to claim 6, wherein the data processing unit, at one time, requests a specified subset A of digits of the security data, and, at another time, requests a specified subset B of digits of the same security data.

20. (previously presented): Method according to claim 17, wherein the step of evaluating whether lack of agreement results from a keying error, or from guessing, comprises the step of

i) requesting further digits, and comparing the further digits with the second data read from the card.

PAGE 9/10 * RCVD AT 12/14/2004 9:47:44 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/0 * DNIS:7467239 * CSID:937 445 6794 * DURATION (mm-ss):03-50